CLAIMS

1. A method for encoding and decoding information, the method comprising the steps of:

(a) using at least one mathematical function;

(b) producing an encryption algorithm using the mathematical functions such that the algorithm has at least two parameters;

(c) defining a decode key of a data stream by defining the value of at least one parameter;

(d) defining information to be carried in a data stream by defining the value of at least one parameter;

(e) producing a data stream using the encryption algorithm and the defined parameter values; and

(f) decrypting the data stream where the decode key is known and used as a constraint in the equation such that the information is available,

wherein the encryption algorithm is selected such that decoding of the encryption algorithm would be ill-conditioned without the constraint.

2. A method according to claim 1 where at least one of the mathematical functions used in the encryption algorithm is selected to be a non-periodic function.

3. A method according to claim 1 or claim 2 where the information includes an authentication key, and including the step of validating the authentication key.

4. A method according to any one of the preceding claims where information includes at least one mutation key, and including the step of using the mutation key to modify the next data stream created or received.

5. A method according to any one the preceding claims where at least the some aspect of the form of ordinate spacing used in the encryption algorithm is effected by at a mutation key.

6. A method according to any one of the preceding claims where the weighting of at least one of the mathematical functions used in the encryption algorithm is effected by a mutation key.

7. A method according to any one of the preceding claims where at the number of mathematical functions used in the encryption algorithm is effected by a mutation key.

8. A method according to any one of the preceding claims where at least the type of mathematical functions used in the encryption algorithm is effected by a mutation key.

9. A method according to any one of the preceding claims and including the step of limiting the accuracy of the representation of the data stream.

10. A method according to claim 9 where the accuracy of representation of the data steam is limited using at least truncation of the values of the data stream.

11. A method according to Claim 9 or Claim 10 where the accuracy of representation of the data steam is limited using at least rounding of values of the data stream.

12. A method according to any one of claims 9 - 11 where the accuracy of representation of the data steam is limited using at least the addition of noise to the data stream.

13. A method according to any one of the preceding claims where the encryption algorithm is selected such that decryption is non-convergent if the decode key and the form of the encryption algorithm are unknown.

14. A method according to any one of the preceding claims where the encryption algorithm is selected such that decryption is non-convergent if where the form of the encryption algorithm is known but the decode key is unknown.

15. A method according to any one of the preceding claims and including the step of the data stream producer decrypting the produced data stream and where decryption fails modifies the value of at least one parameter used to produce said data stream and produces a second data stream and continues the process until a data stream that correctly decrypts has been produced and discards all data streams that could not be decrypted.

16. A method according to claim 15 where the parameters that are altered to allow a data stream that can be decrypted includes at least one mutation parameters.

17. A method according to any one of the preceding claims where the accuracy of representation is such that on average less than 1% of all produced data streams cannot be decrypted.

18. A method according to any one of the preceding claims where the accuracy of representation is such that on average over 10% of all produced data streams cannot be decrypted.

19. A method according to any one of the preceding claims where the accuracy of representation is such that on average over 50% of all produced data streams cannot be decrypted.

20. A method according to any one of the preceding claims and including the step of allowing a user to select a value and influence the probability that produced data streams cannot be decrypted.

21. A method according to any of the preceding claims and including step of sending at least some of the encoded data over a communication link.

22. A method according to any one of the preceding claims and including the step of storing the encoded data in a storage medium.

23. A method according to any one of the preceding claims where at least one of the parameters of the encryption algorithm carries information that may be defined as a password of an external system.

24. A method according to claim 22 where the password is not carried directly but a password mutation key is defined and coded in the parameters to define the changes in a password already held by the receiver and transmitter.

25. A method according to any one of the preceding claims which includes the step of encrypting by conventional means at least some part of an authentication key.

26. A method of claim 25 and including the use of one way encryption.

27. A method according to any one of the preceding claims where the storage area used to hold at least some of the parameter values that form an authentication key is within the same substrate as the processor which encrypts the messages.

28. A method according to any one of the preceding claims which includes the step of including a means to immediately overwrite or flush a temporary data store used in coding or decoding of a data stream.

29. A method according to any one of the preceding claims and including the step of encrypting the produced data stream using conventional encryption means.

30. A method according to any one of the preceding claims and including the step of encrypting at least some of the information prior to it being used to define the values of parameters of the encryption algorithm.

31. A method according to claims 29 and 30 where different encryption algorithms may be used for each separate encryption.

32. A method according to any one of claim 29 - 31 where at least one parameter of the encryption algorithm affects a mutation code for the password of a conventional encryption means.

33. A method according to any one of the preceding claims where authentication between users includes a double handshake protocol.

34. A method according to any one of the preceding claims that includes the step of issuing a unique registration number to each node.

35. A method according to claim 34 where a first decode key is also defined for each node and held securely by the node and on a host such that the host may initiate secure communications with the node after distribution.

36. A method according to claim 35 where each node pair is able to initiate a secure first communication between then by communication with a host and secure transfer of a first decode key code for that node pair by the host.

37. A method according to any one of the preceding claims and including the step of using a protocol such that a first node who is on contact with both a second and third node may act as a start up host between the second and third node without a host and so provide a distributed start up means.

38. A method according to any one of the preceding claims and including a step of having a plurality of stored starting decode keys between node pairs on each node such that on a communication failure reconnection may occur rapidly.

39. A method according to any one of the preceding claims in which the method is used in nested mode such that a first encryption algorithm is used to authenticate between users and then a second encryption algorithm is used to transfer useful information.

40. A method according to any one of the preceding claims where the information stored includes that of tokens of value that become the property of the owner of the registration number due to a purchase made by means of the invention where the tokens may be exchanged for further goods or services.

41. A method according to any one of the preceding claims that allows a encryption method where the time taken to trail a single guess of a password is significantly longer than the time taken to validate the correct password.

42. Apparatus comprising transmitting means, receiving means, processing means and operating instructions allowing decryption of a signal according to the method of any one of the preceding claims.

43. Apparatus comprising writing means, reading means, processing means and operating instructions allowing decryption of a signal according to the method of any one of claims 1 – 41.